Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/001211

International filing date: 28 January 2005 (28.01.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-023335
Filing date: 30 January 2004 (30.01.2004)

Date of receipt at the International Bureau: 14 April 2005 (14.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

日本国特許庁
JAPAN PATENT OFFICE

22.02.2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

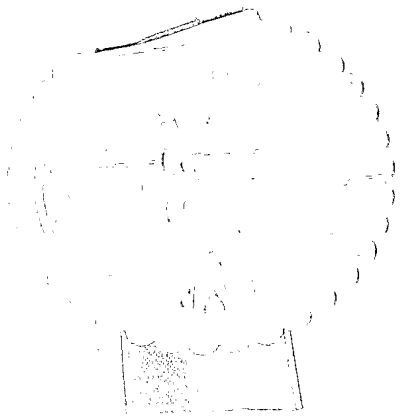
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００４年　１月３０日

出願番号
Application Number: 特願２００４－０２３３３５

[ST. 10/C]: ［ＪＰ２００４－０２３３３５］

出願人
Applicant(s): 日本ビクター株式会社



２００５年　３月３１日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００５－３０２８２９３

【書類名】　特許願
【整理番号】　415001145
【提出日】　平成16年 1月30日
【あて先】　特許庁長官殿
【国際特許分類】　G09C　1/00
H03K　3/84
H04L　9/24
【発明者】
【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内
【氏名】　猪羽　渉
【発明者】
【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内
【氏名】　日暮　誠司
【特許出願人】
【識別番号】　000004329
【氏名又は名称】　日本ビクター株式会社
【代理人】
【識別番号】　100083806
【弁理士】
【氏名又は名称】　三好　秀和
【電話番号】　03-3504-3075
【選任した代理人】
【識別番号】　100068342
【弁理士】
【氏名又は名称】　三好　保男
【選任した代理人】
【識別番号】　100101247
【弁理士】
【氏名又は名称】　高橋　俊一
【手数料の表示】
【予納台帳番号】　001982
【納付金額】　21,000円
【提出物件の目録】
【物件名】　特許請求の範囲　1
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9802012

【書類名】特許請求の範囲
【請求項１】
所定のビット長の擬似乱数列を生成する擬似乱数生成装置であって、
ｍ段のシフトレジスタを有し、所定のビット長のビット列を出力する第１の線形フィードバックシフトレジスタと、
ｎ段のシフトレジスタを有し、所定のビット長のビット列を出力する第２の線形フィードバックシフトレジスタと、
所定の条件に従って、前記第１の線形フィードバックシフトレジスタおよび前記第２の線形フィードバックシフトレジスタを構成する各シフトレジスタの初期値を生成し、それぞれの当該初期値を前記第１の線形フィードバックシフトレジスタおよび前記第２の線形フィードバックシフトレジスタへ供給する初期値生成手段と、
所定の条件に従って、前記第２の線形フィードバックシフトレジスタの特性多項式の係数を生成し、前記第２の線形フィードバックシフトレジスタへ供給する多項式係数生成手段と、
前記第１の線形フィードバックシフトレジスタの特性多項式として原始多項式を前記原始多項式より少ない情報量の識別番号と共に複数記憶する原始多項式記憶手段と、
所定の条件に従って、前記原始多項式記憶手段に記憶されている原始多項式を１つ選択し、その原始多項式の係数を特性多項式の係数として前記第１の線形フィードバックシフトレジスタへ供給する原始多項式選択手段と、
前記第１の線形フィードバックシフトレジスタから出力されるビット列と、および前記第２の線形フィードバックシフトレジスタから出力されるビット列とに基づいて、各ビットの論理演算から所定のビット長の擬似乱数列を生成し、出力する擬似乱数出力手段と、
を備えることを特徴とする擬似乱数生成装置。
【請求項２】
前記擬似乱数生成装置は、
前記原始多項式選択手段によって選択された前記原始多項式の識別番号、前記初期値生成手段によって生成された前記第１の線形フィードバックシフトレジスタおよび前記第２の線形フィードバックシフトレジスタを構成する各シフトレジスタの初期値、前記多項式係数生成手段によって生成された前記特性多項式の係数のそれぞれからなるイニシャルデータを生成、当該イニシャルデータを他の擬似乱数生成装置へ送出し、当該イニシャルデータを他の擬似乱数生成装置から受信した場合は、当該イニシャルデータから前記第１のフィードバックシフトレジスタと前記第２のフィードバックシフトレジスタとの各初期値を抽出して前記第１の線形フィードバックシフトレジスタと前記第２の線形フィードバックシフトレジスタに供給し、当該イニシャルデータから前記特性多項式の係数を抽出して前記第２の線形フィードバックシフトレジスタへ供給し、当該イニシャルデータから前記原始多項式の識別番号を抽出して前記原始多項式選択手段に供給する通信手段を備え、
前記原始多項式選択手段は、前記通信手段によって抽出された前記識別番号を基に、前記原始多項式記憶手段に記憶されている原始多項式を１つ選択し、その原始多項式の係数を前記第１の線形フィードバックシフトレジスタへ供給する手段であることを特徴とする請求項１に記載の擬似乱数生成装置。
【請求項３】
所定のビット長の擬似乱数列を生成するコンピュータによって実行される擬似乱数生成プログラムであって、
当該擬似乱数生成プログラムは、前記コンピュータを
ｍ段のシフトレジスタを有し、所定のビット長のビット列を出力する第１の線形フィードバックシフトレジスタと、
ｎ段のシフトレジスタを有し、所定のビット長のビット列を出力する第２の線形フィードバックシフトレジスタと、
所定の条件に従って、前記第１の線形フィードバックシフトレジスタおよび前記第２の線形フィードバックシフトレジスタを構成する各シフトレジスタの初期値を生成し、それ

ぞれの当該初期値を前記第１の線形フィードバックシフトレジスタおよび前記第２の線形フィードバックシフトレジスタへ供給する初期値生成手段と、
所定の条件に従って、前記第２の線形フィードバックシフトレジスタの特性多項式の係数を生成し、前記第２の線形フィードバックシフトレジスタへ供給する多項式係数生成手段と、
前記第１の線形フィードバックシフトレジスタの特性多項式として原始多項式を前記原始多項式より少ない情報量の識別番号と共に複数記憶する原始多項式記憶手段と、
所定の条件に従って、前記原始多項式記憶手段に記憶されている原始多項式を１つ選択し、その原始多項式の係数を特性多項式の係数として前記第１の線形フィードバックシフトレジスタへ供給する原始多項式選択手段と、
前記第１の線形フィードバックシフトレジスタから出力されるビット列と、および前記第２の線形フィードバックシフトレジスタから出力されるビット列とに基づいて、各ビットの論理演算から所定のビット長の擬似乱数列を生成し、出力する擬似乱数出力手段と、
して機能させることを特徴とする擬似乱数生成プログラム。
【請求項４】
前記擬似乱数生成プログラムは、前記コンピュータを
前記原始多項式選択手段によって選択された前記原始多項式の識別番号、前記初期値生成手段によって生成された前記第１の線形フィードバックシフトレジスタおよび前記第２の線形フィードバックシフトレジスタを構成する各シフトレジスタの初期値、前記多項式係数生成手段によって生成された前記特性多項式の係数のそれぞれからなるイニシャルデータを生成、当該イニシャルデータを他の擬似乱数生成装置へ送出し、当該イニシャルデータを他の擬似乱数生成装置から受信した場合は、当該イニシャルデータから前記第１のフィードバックシフトレジスタと前記第２のフィードバックシフトレジスタとの各初期値を抽出して前記第１の線形フィードバックシフトレジスタと前記第２の線形フィードバックシフトレジスタに供給し、当該イニシャルデータから前記特性多項式の係数を抽出して前記第２の線形フィードバックシフトレジスタへ供給し、当該イニシャルデータから前記原始多項式の識別番号を抽出して前記原始多項式選択手段に供給する通信手段としても機能させ、
前記原始多項式選択手段は、前記通信手段によって抽出された前記識別番号を基に、前記原始多項式記憶手段に記憶されている原始多項式を１つ選択し、その原始多項式の係数を前記第１の線形フィードバックシフトレジスタへ供給する手段であることを特徴とする請求項３に記載の擬似乱数生成プログラム。

【書類名】明細書
【発明の名称】擬似乱数生成装置および擬似乱数生成プログラム
【技術分野】
【０００１】
本発明は、暗号通信に利用される擬似乱数を生成する擬似乱数生成装置および擬似乱数生成プログラムに関する。
【背景技術】
【０００２】
現在、電話や無線、インターネット等におけるデータ通信では、通信されるデータを第三者による盗聴や改ざんから保護するために、データの暗号化が行われている。データの送信側では、暗号鍵を用いて送信するデータを暗号化した後送信し、受信側では、その暗号化されたデータを受信すると、復号鍵を用いて復号化しデータを得ている。もしこの時、第三者がデータを傍受しても、正当な復号鍵を持たないため暗号化されたデータを復号することができず、また、意図したデータの改ざんを行うこともできない。
【０００３】
このような暗号化の方式には、共通鍵暗号方式や公開鍵暗号方式があり、それぞれの特徴をいかして利用される条件に応じて選択される。いずれの方式であっても、暗号鍵によって通信されるデータの安全性が保障されており、その暗号鍵は容易に推測されないように擬似乱数を用いる方法が知られている。
【０００４】
例えば、線形フィードバックシフトレジスタによる擬似乱数の生成方法では、乱数生成のための比較的短い初期値からデータ長の長い擬似乱数列を生成することができるため、複数の装置で同じ擬似乱数を生成しようとするとき、初期値を共有するだけで良い。また、一般に、特定の条件を満たす原始多項式を特性多項式とする複数の線形フィードバックシフトレジスタを組み合わせることで、生成される擬似乱数の予測が困難な擬似乱数生成装置を実現可能なことが知られている。さらに、初期値を共有しなくても、複数の線形フィードバックシフトレジスタの選択情報を共有化することで、同じ擬似乱数列を生成することも可能である（特許文献１）。
【０００５】
しかしながら、線形フィードバックシフトレジスタを用いた擬似乱数生成装置では、たとえ非線形な処理を組み合わせた方法であっても、ある特定のアルゴリズムで擬似乱数が生成されるため、初期値や生成される擬似乱数列の一部からその後生成される擬似乱数が推測される恐れがあった。
【０００６】
また、複数の線形フィードバックシフトレジスタからいくつかのレジスタを選択して擬似乱数を生成する場合には、生成される擬似乱数列の推測は困難になるものの、任意の係数を特性多項式とする線形フィードバックシフトレジスタを組み合わせると、生成される擬似乱数列が必ずしもＭ系列（Maximal-length sequences）とはならずに、短い周期で同じ擬似乱数列を繰り返し生成してしまうという問題があるため、予め特定の条件を満たす多項式を多数用意した中から選択して組み合わせる必要があった。これは実際の処理では、常に利用するわけではない線形フィードバックシフトレジスタを実装する必要があり効率的ではなかった。
【特許文献１】特開平１０－９１０６６号公報
【特許文献２】特開平１０－９３５４８号公報
【特許文献３】特開２０００－８１９６９号公報
【発明の開示】
【発明が解決しようとする課題】
【０００７】
本発明は、生成される擬似乱数列や送受信されるデータを観測されても、その後生成される擬似乱数列の推測が困難な暗号通信に好適な擬似乱数生成装置および擬似乱数生成プ

ログラムを提供することを目的とする。

【課題を解決するための手段】

【０００８】

上記目的を達成するために、請求項１に記載の擬似乱数生成装置は、所定のビット長の擬似乱数列を生成する擬似乱数生成装置であって、ｍ段のシフトレジスタを有し、所定のビット長のビット列を出力する第１の線形フィードバックシフトレジスタと、ｎ段のシフトレジスタを有し、所定のビット長のビット列を出力する第２の線形フィードバックシフトレジスタと、所定の条件に従って、前記第１の線形フィードバックシフトレジスタおよび前記第２の線形フィードバックシフトレジスタを構成する各シフトレジスタの初期値を生成し、それぞれの当該初期値を前記第１の線形フィードバックシフトレジスタおよび前記第２の線形フィードバックシフトレジスタへ供給する初期値生成手段と、所定の条件に従って、前記第２の線形フィードバックシフトレジスタの特性多項式の係数を生成し、前記第２の線形フィードバックシフトレジスタへ供給する多項式係数生成手段と、前記第１の線形フィードバックシフトレジスタの特性多項式として原始多項式を前記原始多項式より少ない情報量の識別番号と共に複数記憶する原始多項式記憶手段と、所定の条件に従って、前記原始多項式記憶手段に記憶されている原始多項式を１つ選択し、その原始多項式の係数を特性多項式の係数として前記第１の線形フィードバックシフトレジスタへ供給する原始多項式選択手段と、前記第１の線形フィードバックシフトレジスタから出力されるビット列と、および前記第２の線形フィードバックシフトレジスタから出力されるビット列とに基づいて、各ビットの論理演算から所定のビット長の擬似乱数列を生成し、出力する擬似乱数出力手段とを備えることを特徴とする。

【０００９】

また、請求項２に記載の擬似乱数生成装置は、請求項１に記載の擬似乱数生成装置であって、前記擬似乱数生成装置は、前記原始多項式選択手段によって選択された前記原始多項式の識別番号、前記初期値生成手段によって生成された前記第１の線形フィードバックシフトレジスタおよび前記第２の線形フィードバックシフトレジスタを構成する各シフトレジスタの初期値、前記多項式係数生成手段によって生成された前記特性多項式の係数のそれぞれからなるイニシャルデータを生成、当該イニシャルデータを他の擬似乱数生成装置へ送出し、当該イニシャルデータを他の擬似乱数生成装置から受信した場合は、当該イニシャルデータから前記第１のフィードバックシフトレジスタと前記第２のフィードバックシフトレジスタとの各初期値を抽出して前記第１の線形フィードバックシフトレジスタと前記第２の線形フィードバックシフトレジスタに供給し、当該イニシャルデータから前記特性多項式の係数を抽出して前記第２の線形フィードバックシフトレジスタへ供給し、当該イニシャルデータから前記原始多項式の識別番号を抽出して前記原始多項式選択手段に供給する通信手段を備え、前記原始多項式選択手段は、前記通信手段によって抽出された前記識別番号を基に、前記原始多項式記憶手段に記憶されている原始多項式を１つ選択し、その原始多項式の係数を前記第１の線形フィードバックシフトレジスタへ供給する手段であることを特徴とする。

【００１０】

また、請求項３に記載の擬似乱数生成プログラムは、所定のビット長の擬似乱数列を生成するコンピュータによって実行される擬似乱数生成プログラムであって、当該擬似乱数生成プログラムは、前記コンピュータをｍ段のシフトレジスタを有し、所定のビット長のビット列を出力する第１の線形フィードバックシフトレジスタと、ｎ段のシフトレジスタを有し、所定のビット長のビット列を出力する第２の線形フィードバックシフトレジスタと、所定の条件に従って、前記第１の線形フィードバックシフトレジスタおよび前記第２の線形フィードバックシフトレジスタを構成する各シフトレジスタの初期値を生成し、それぞれの当該初期値を前記第１の線形フィードバックシフトレジスタおよび前記第２の線形フィードバックシフトレジスタへ供給する初期値生成手段と、所定の条件に従って、前記第２の線形フィードバックシフトレジスタの特性多項式の係数を生成し、前記第２の線形フィードバックシフトレジスタへ供給する多項式係数生成手段と、前記第１の線形フィ

ードバックシフトレジスタの特性多項式として原始多項式を前記原始多項式より少ない情報量の識別番号と共に複数記憶する原始多項式記憶手段と、所定の条件に従って、前記原始多項式記憶手段に記憶されている原始多項式を１つ選択し、その原始多項式の係数を特性多項式の係数として前記第１の線形フィードバックシフトレジスタへ供給する原始多項式選択手段と、前記第１の線形フィードバックシフトレジスタから出力されるビット列と、および前記第２の線形フィードバックシフトレジスタから出力されるビット列とに基づいて、各ビットの論理演算から所定のビット長の擬似乱数列を生成し、出力する擬似乱数出力手段として機能させることを特徴とする。

【００１１】

また、請求項４に記載の擬似乱数生成プログラムは、請求項３に記載の擬似乱数生成プログラムであって、前記擬似乱数生成プログラムは、前記コンピュータを前記原始多項式選択手段によって選択された前記原始多項式の識別番号、前記初期値生成手段によって生成された前記第１の線形フィードバックシフトレジスタおよび前記第２の線形フィードバックシフトレジスタを構成する各シフトレジスタの初期値、前記多項式係数生成手段によって生成された前記特性多項式の係数のそれぞれからなるイニシャルデータを生成、当該イニシャルデータを他の擬似乱数生成装置へ送出し、当該イニシャルデータを他の擬似乱数生成装置から受信した場合は、当該イニシャルデータから前記第１のフィードバックシフトレジスタと前記第２のフィードバックシフトレジスタとの各初期値を抽出して前記第１の線形フィードバックシフトレジスタと前記第２の線形フィードバックシフトレジスタに供給し、当該イニシャルデータから前記特性多項式の係数を抽出して前記第２の線形フィードバックシフトレジスタへ供給し、当該イニシャルデータから前記原始多項式の識別番号を抽出して前記原始多項式選択手段に供給する通信手段としても機能させ、前記原始多項式選択手段は、前記通信手段によって抽出された前記識別番号を基に、前記原始多項式記憶手段に記憶されている原始多項式を１つ選択し、その原始多項式の係数を前記第１の線形フィードバックシフトレジスタへ供給する手段であることを特徴とする。

【発明の効果】

【００１２】

本発明によれば、常に所定のＭ系列より長い周期の擬似乱数列を生成することが可能となり、初期値だけでなく、特性多項式の係数も任意に設定できるため、生成された擬似乱数列を観測されてもその後生成される擬似乱数列を推測することは困難であり、生成される擬似乱数列の安全性を確保することができ、通信されるデータの安全性が保障される。

【００１３】

また、第１の線形フィードバックシフトレジスタの特性多項式として設定される原始多項式の選択には、その識別情報を用いることにより、係数を送受信するより少ないデータ量で済む。

【発明を実施するための最良の形態】

【００１４】

本発明の実施形態を、図１～図９を用いて説明する。なお、擬似乱数生成装置１が生成する擬似乱数のビット長をｈ＋１とする。

【００１５】

≪第１の実施形態≫

第１の実施形態における擬似乱数生成装置１は、図１に示すように、第１線形フィードバックシフトレジスタ２、第２線形フィードバックシフトレジスタ３、初期値生成部４、多項式係数生成部５、および擬似乱数出力部６を有する。

【００１６】

第１線形フィードバックシフトレジスタ２は、ｍ次の線形フィードバックシフトレジスタであり、ｍ個のフリップフロップ回路を有する（詳細については後述）。また、第２線形フィードバックシフトレジスタ３は、ｎ次の線形フィードバックシフトレジスタであり、ｎ個のフリップフロップ回路を有する（詳細については後述）。

【００１７】

初期値生成部４は、外部から入力される初期情報、あるいは予め定められた所定の条件、例えば、日時情報のように常に変化する情報や熱雑音等の物理現象を利用して得られる条件に従って、第１線形フィードバックシフトレジスタ２を構成する各フリップフロップの初期値ia（$ia_{m-1}, ia_{m-2}, \cdots, ia_1, ia_0$）を生成し、第１線形フィードバックシフトレジスタ２へ供給する機能、第２線形フィードバックシフトレジスタ３を構成する各フリップフロップの初期値ib（$ib_{n-1}, ib_{n-2}, \cdots, ib_1, ib_0$）を生成し、第２線形フィードバックシフトレジスタ３へ供給する機能を有する。ただし、第２線形フィードバックシフトレジスタ３からの出力が常に“0”にならないよう、少なくとも初期値ia_{m-1}～ia_0のいずれか１つが値“1”であり、同様に、少なくとも初期値ib_{n-1}～ib_0のいずれか１つが値“1”であることとする。

【００１８】

また、多項式係数生成部５は、外部から入力される初期情報、あるいは予め定められた所定の条件、例えば、日時情報のように常に変化する情報や熱雑音等の物理現象を利用して得られる条件に従って、第２線形フィードバックシフトレジスタ３の特性多項式の係数s（$s_{n-1}, s_{n-2}, \cdots, s_2, s_1$）を生成し、第２線形フィードバックシフトレジスタ３へ供給する機能を有する。

【００１９】

また、擬似乱数出力部６は、第１線形フィードバックシフトレジスタ２から順次出力されるビット列ra（$ra_0, ra_1, \cdots, ra_{h-1}, ra_h$）と、および第２線形フィードバックシフトレジスタ３から順次出力されるビット列rb（$rb_0, rb_1, \cdots, rb_{h-1}, rb_h$）とに基づいて、各ビットの排他的論理和を求め所定のビット長の擬似乱数r（$r_0, r_1, \cdots, r_{h-1}, r_h$）を生成し、出力する機能を有する。

【００２０】

第１線形フィードバックシフトレジスタ２は、図２に示すように、ｍ個のフリップフロップ回路とＡＮＤ回路、およびＸＯＲ回路から構成される。この第１線形フィードバックシフトレジスタ２の特性多項式は、予め定められた原始多項式$a_m x^m + a_{m-1} x^{m-1} + a_{m-2} x^{m-2} + \cdots + a_2 x^2 + a_1 x + a_0$（ただし、$a_m=1$）であり、ＡＮＤ回路それぞれに原始多項式の係数a（$a_{m-1}, \cdots, a_1$）が設定される。

【００２１】

従って、$a_i=0$（$0<i<m$）の時は、フリップフロップFA_{i-1}（$0<i<m$）から出力される値に関係なくＡＮＤ回路からは“0”が出力され、$a_i=1$（$0<i<m$）の時は、フリップフロップFA_{i-1}（$0<i<m$）から出力される値が出力される。

【００２２】

第２線形フィードバックシフトレジスタ３は、図３に示すように、ｎ個のフリップフロップ回路とＡＮＤ回路、およびＸＯＲ回路から構成される。この第２線形フィードバックシフトレジスタ３の特性多項式を$b_n x^n + b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \cdots + b_2 x^2 + b_1 x + b_0$とすると、ＡＮＤ回路それぞれに特性多項式の係数b（$b_{n-1}, \cdots, b_1$=係数s）が設定される。

【００２３】

従って、$b_j=0$（$0<j<n$）の時は、フリップフロップFB_{j-1}（$0<j<n$）から出力される値に関係なくＡＮＤ回路からは“0”が出力され、$b_j=1$（$0<j<n$）の時は、フリップフロップFB_{j-1}（$0<j<n$）から出力される値が出力される。

【００２４】

次に、擬似乱数生成装置１Ａの動作について、図４のフローチャートに基づいて説明する。

【００２５】

擬似乱数生成装置１Ａが擬似乱数生成の処理を開始すると、まず、初期値生成部４が、外部から入力される初期情報、あるいは予め定められた所定の条件に従って、初期値ia（$ia_{m-1}, ia_{m-2}, \cdots, ia_1, ia_0$）と初期値ib（$ib_{n-1}, ib_{n-2}, \cdots, ib_1, ib_0$）を生成し（ステップＳ０１）、それぞれの初期値を第１線形フィードバックシフトレジスタ２と第２線形フィードバックシフトレジスタ３へ供給する。

【００２６】
また、多項式係数生成部５が、外部から入力される初期情報、あるいは予め定められた所定の条件に従って、第２線形フィードバックシフトレジスタ３の特性多項式の係数s（$s_{n-1}, s_{n-2}, \cdots, s_2, s_1$）を生成し（ステップＳ０２）、第２線形フィードバックシフトレジスタ３へ供給する。
【００２７】
第１線形フィードバックシフトレジスタ２と第２線形フィードバックシフトレジスタ３は、初期値生成部４と多項式係数生成部５から各初期値と係数が供給されると、各フリップフロップ回路とＡＮＤ回路に各初期値と係数を設定し、出力ビット数をカウントするカウンタｋの値をｋ＝０に設定する（ステップＳ０３）。第１線形フィードバックシフトレジスタ２の各フリップフロップ回路$FA_{m-1}, FA_{m-2}, \cdots, FA_1, FA_0$には、初期値ia（$ia_{m-1}, ia_{m-2}, \cdots, ia_1, ia_0$）が設定され、各ＡＮＤ回路には、原始多項式の係数a（$a_{m-1}, \cdots, a_1$）が設定される。また、第２線形フィードバックシフトレジスタ３の各フリップフロップ回路$FB_n, FB_{n-1}, \cdots, FB_1, FB_0$には、初期値ib（$ib_{n-1}, ib_{n-2}, \cdots, ib_1, ib_0$）が設定され、各ＡＮＤ回路には、特性多項式の係数s（$s_{n-1}, s_{n-2}, \cdots, s_2, s_1$）が設定される。なお、図３の第２線形フィードバックシフトレジスタ３では、$b_n=1, b_0=1$としているが、b_nおよびb_0にＡＮＤ回路を設けて、他の係数と同様に任意の値を設定できるようにしてもよい。
【００２８】
次に、第１線形フィードバックシフトレジスタ２にクロック信号を入力すると（ステップＳ０４）、第１線形フィードバックシフトレジスタ２は演算を行い、ビットra_kを出力する（ステップＳ０５）。同様に、第２線形フィードバックシフトレジスタ３にクロック信号を入力すると（ステップＳ０６）、第２線形フィードバックシフトレジスタ３は演算を行い、ビットrb_kを出力する（ステップＳ０７）。
【００２９】
擬似乱数出力部６は、第１線形フィードバックシフトレジスタ２からビットra_kが出力され、第２線形フィードバックシフトレジスタ３からビットrb_kが出力されると、両ビット値の排他的論理和を求めビットr_kを生成する（ステップＳ０８）。
【００３０】
次に、第１線形フィードバックシフトレジスタ２と第２線形フィードバックシフトレジスタ３は、カウンタｋの値を１つインクリメント（ｋ←ｋ＋１）し（ステップＳ０９）、カウンタｋの値がｈの値を超えたかどうか判定する（ステップＳ１０）。カウンタｋの値がｈ以下の場合は、第１線形フィードバックシフトレジスタ２はステップＳ０４に戻ってビットra_{k+1}を出力し、第２線形フィードバックシフトレジスタ３はステップＳ０６に戻ってビットrb_{k+1}を出力し、擬似乱数出力部６は、ビットr_{k+1}を生成する。
【００３１】
カウンタｋの値がｈより大きい場合は、擬似乱数生成装置１は擬似乱数生成処理を終了し、これまでに生成されたビット$r_0, r_1, \cdots, r_{h-1}, r_h$が擬似乱数r（$r_0, r_1, \cdots, r_{h-1}, r_h$）として出力される（ステップＳ１１）。
【００３２】
ここで、図５を用いて具体的に説明する。一例として、８ビットの擬似乱数rを出力するものとし、第１線形フィードバックシフトレジスタ２の原始多項式をx^7+x^3+1とし、第１線形フィードバックシフトレジスタ２のフリップフロップ回路を７段構成として初期値ia（$ia_6, ia_5, \cdots, ia_1, ia_0$）＝（1,0,1,0,1,0,1）、第２線形フィードバックシフトレジスタ３のフリップフロップ回路を８段構成として初期値ib（$ib_7, ib_6, \cdots, ib_1, ib_0$）＝（1,1,1,1,0,0,0,0）、第２線形フィードバックシフトレジスタ３の特性多項式の係数s（$s_7, s_6, \cdots, s_2, s_1$）＝（0,1,1,1,0,1,1）がそれぞれ設定されたとする。
【００３３】
まず、１回目のクロック信号が入力されると、第１線形フィードバックシフトレジスタ２においては、$FA_0 \rightarrow FA_1$、$FA_1 \rightarrow FA_2$、…、$FA_5 \rightarrow FA_6$とビットがシフトして（$FA_6, FA_5, FA_4, FA_3, FA_2, FA_1$）＝（0,1,0,1,0,1）となる。第１線形フィードバックシフトレジスタ２の原

始多項式をx^7+x^3+1なので、FA_6のビット“1”はFA_2からFA_3へ出力されるビット“1”との排他的論理和“0”をFA_0にフィードバックして図５の+1の状態になり、第１線形フィードバックシフトレジスタ２は“0”をra_0として出力する。

【００３４】

また、１回目のクロック信号が入力されると、第２線形フィードバックシフトレジスタ３においては、$FB_0 \rightarrow FB_1$、$FB_1 \rightarrow FB_2$、…、$FB_6 \rightarrow FB_7$とビットがシフトして（$FB_7, FB_6, FB_5, FB_4, FB_3, FB_2, FB_1$）＝（1,1,1,0,0,0,0）となる。特性多項式の係数s（$s_7, s_6, \cdots, s_2, s_1$）＝（0,1,1,1,0,1,1）から、特性多項式は$x^8+x^6+x^5+x^4+x^2+x+1$なので、FB_5からFB_6へ出力されるビット“1”と、FB_3からFB_4へ出力されるビット“0”と、FB_1からFB_2へ出力されるビット“0”と、FB_0からFB_1へ出力されるビット“0” との排他的論理和“1”をFB_0にフィードバックして図５の+1の状態になり、第２線形フィードバックシフトレジスタ３は“1”をrb_0として出力する。

【００３５】

２回目のクロック信号が入力されると、第１線形フィードバックシフトレジスタ２および第２線形フィードバックシフトレジスタ３は、同様にビットシフトを行い、原始多項式と特性多項式に基づいてフィードバックを行い、図５の+2の状態となり、それぞれ$ra_1=0$および $rb_1=1$を出力する。

【００３６】

このように演算を繰り返すことによって、第１線形フィードバックシフトレジスタ２からは（$ra_0, ra_1, \cdots, ra_6, ra_7$）＝（0,0,0,0,1,0,1,1）、第２線形フィードバックシフトレジスタ３からは（$rb_0, rb_1, \cdots, rb_6, rb_7$）＝（1,1,1,1,1,0,0,1）が出力され、（$ra_0, ra_1, \cdots, ra_6, ra_7$）＝（0,0,0,0,1,0,1,1）と（$rb_0, rb_1, \cdots, rb_6, rb_7$）＝（1,1,1,1,1,0,0,1）との排他的論理和から擬似乱数r（$r_0, r_1, \cdots, r_6, r_7$）＝（1,1,1,1,0,0,1,0）が出力される。

【００３７】

≪第２の実施形態≫

第２の実施形態における擬似乱数生成装置１Ｂは、図６に示すように、第１線形フィードバックシフトレジスタ２、第２線形フィードバックシフトレジスタ３、初期値生成部４、多項式係数生成部５、擬似乱数出力部６、原始多項式選択部７、および原始多項式記憶部８を有する。なお、第１の実施形態と同じものについては、同じ番号を付し、その詳細な説明を省略する。

【００３８】

原始多項式選択部７は、外部から入力される初期情報に従って、原始多項式記憶部８に記憶されている原始多項式を１つ選択し、特性多項式としてその原始多項式の係数a（$a_{m-1}, \cdots, a_1$）を第１線形フィードバックシフトレジスタ２へ供給する機能を有する。

【００３９】

原始多項式記憶部８は、第１線形フィードバックシフトレジスタ２の各ＡＮＤ回路を設定するための原始多項式を識別番号と共に複数記憶する。この識別番号によって、原始多項式の係数より少ない情報量で各ＡＮＤ回路を設定することが可能であり、例えば、図６に示すように、ビット長を２ビットとすると、原始多項式記憶部８は、識別番号No.“00”はx^7+x^3+1、識別番号No.“01”は$x^7+x^3+x^2+x+1$、識別番号No.“10”は$x^7+x^4+x^3+x^2+1$、識別番号No.“11”は$x^7+x^6+x^5+x^4+x^2+x+1$というような原始多項式を記憶する。

【００４０】

次に、擬似乱数生成装置１Ｂの動作について、図７のフローチャートに基づいて説明する。

【００４１】

擬似乱数生成装置１Ｂが擬似乱数生成の処理を開始すると、まず、原始多項式選択部７が、外部から入力される初期情報に従って、原始多項式記憶部８から原始多項式を１つ選択し（ステップＳ２１）、その選択した原始多項式の係数を特性多項式の係数a（$a_{m-1}, \cdots, a_1$）として第１線形フィードバックシフトレジスタ２へ供給する。

【００４２】

また、初期値生成部４は、外部から入力される初期情報、あるいは予め定められた所定の条件に従って、初期値ia（$ia_{m-1}, ia_{m-2}, \cdots, ia_1, ia_0$）と初期値ib（$ib_{n-1}, ib_{n-2}, \cdots, ib_1, ib_0$）を生成し（ステップＳ２２）、それぞれの初期値を第１線形フィードバックシフトレジスタ２と第２線形フィードバックシフトレジスタ３へ供給する。

【００４３】

また、多項式係数生成部５が、外部から入力される初期情報、あるいは予め定められた所定の条件に従って、第２線形フィードバックシフトレジスタ３の特性多項式の係数s（$s_{n-1}, s_{n-2}, \cdots, s_2, s_1$）を生成し（ステップＳ２３）、第２線形フィードバックシフトレジスタ３へ供給する。

【００４４】

第１線形フィードバックシフトレジスタ２と第２線形フィードバックシフトレジスタ３は、原始多項式選択部７、初期値生成部４、および多項式係数生成部５から各初期値と係数が供給されると、各フリップフロップ回路とＡＮＤ回路に各初期値と係数を設定し、出力ビット数をカウントするカウンタｋの値をｋ＝０に設定する（ステップＳ２４）。第１線形フィードバックシフトレジスタ２の各フリップフロップ回路$FA_{m-1}, FA_{m-2}, \cdots, FA_1, FA_0$には、初期値ia（$ia_{m-1}, ia_{m-2}, \cdots, ia_1, ia_0$）が設定され、各ＡＮＤ回路には、原始多項式選択部７から供給された特性多項式の係数a（$a_{m-1}, \cdots, a_1$）が設定される。また、第２線形フィードバックシフトレジスタ３の各フリップフロップ回路$FB_{n-1}, FB_{n-2}, \cdots, FB_1, FB_0$には、初期値ib（$ib_{n-1}, ib_{n-2}, \cdots, ib_1, ib_0$）が設定され、各ＡＮＤ回路には、特性多項式の係数s（$s_{n-1}, s_{n-2}, \cdots, s_2, s_1$）が設定される。なお、図３の第２線形フィードバックシフトレジスタ３では、$b_n=1, b_0=1$としているが、b_nおよびb_0にＡＮＤ回路を設けて、他の係数と同様に任意の値を設定できるようにしてもよい。

【００４５】

以降、第１の実施形態（ステップＳ０４～ステップＳ１１）と同様の処理を行って擬似乱数r（$r_0, r_1, \cdots, r_{h-1}, r_h$）を出力する（ステップＳ２５～ステップＳ３２）。

【００４６】

≪第３の実施形態≫

第３の実施形態として、２つの擬似乱数生成装置１、例えば送信装置側に設けられた擬似乱数生成装置１と受信装置側に設けられた擬似乱数生成装置１とで特性多項式の係数と初期値（イニシャルデータ）を共有して、同じ擬似乱数を生成する擬似乱数生成装置１Ｃを示す。

【００４７】

第３の実施形態における擬似乱数生成装置１Ｃは、図８に示すように、第１線形フィードバックシフトレジスタ２、第２線形フィードバックシフトレジスタ３、初期値生成部４、多項式係数生成部５、擬似乱数出力部６、原始多項式選択部７、原始多項式記憶部８、および通信部９を有する。なお、第１の実施形態および第２の実施形態と同じものについては、同じ番号を付し、その詳細な説明を省略する。また、便宜的に、イニシャルデータ送信側の擬似乱数生成装置１の構成要件には“ｔ”の文字を、イニシャルデータ受信側の擬似乱数生成装置１の構成要件には“ｒ”の文字を付す。

【００４８】

通信部９は、原始多項式選択部７が選択した原始多項式の識別番号、初期値生成部４が生成した初期値ia（$ia_{m-1}, ia_{m-2}, \cdots, ia_1, ia_0$）および初期値ib（$ib_{n-1}, ib_{n-2}, \cdots, ib_1, ib_0$）、多項式係数生成部５が生成した特性多項式の係数s（$s_{n-1}, s_{n-2}, \cdots, s_2, s_1$）を基に、原始多項式の識別番号、特性多項式の係数の初期値、および各初期値のそれぞれのビット列からなるイニシャルデータを生成する機能、およびそのイニシャルデータを他の擬似乱数生成装置１と送受信する機能を有する。

【００４９】

また、通信部９は、イニシャルデータを受信した場合は、イニシャルデータから初期値ib（$ib_{n-1}, ib_{n-2}, \cdots, ib_1, ib_0$）と特性多項式の係数s（$s_{n-1}, s_{n-2}, \cdots, s_2, s_1$）とを抽出し、第２線形フィードバックシフトレジスタ３に供給する機能、イニシャルデータから初期

値ia（$ia_{m-1}, ia_{m-2}, \cdots, ia_1, ia_0$）を抽出し、第１線形フィードバックシフトレジスタ２に供給する機能、イニシャルデータから原始多項式の識別番号を抽出し、原始多項式選択部７に供給する機能を有する。

【００５０】

次に、２つの擬似乱数生成装置１Ｃで同じ擬似乱数を生成する際の動作について、図９のシーケンス図に基づいて説明する。

【００５１】

擬似乱数生成装置１Ｃｔが擬似乱数生成の処理を開始すると、まず、原始多項式選択部７ｔが、外部から入力される初期情報に従って、原始多項式記憶部８ｔから原始多項式を１つ選択し（ステップＳ４１）、その選択した原始多項式の係数を特性多項式の係数a（$a_{m-1}, \cdots, a_1$）として第１線形フィードバックシフトレジスタ２ｔへ供給すると共に、通信部９ｔへ原始多項式の識別番号を供給する。

【００５２】

また、初期値生成部４ｔは、外部から入力される初期情報、あるいは予め定められた所定の条件に従って、初期値ia（$ia_{m-1}, ia_{m-2}, \cdots, ia_1, ia_0$）と初期値ib（$ib_{n-1}, ib_{n-2}, \cdots, ib_1, ib_0$）を生成し（ステップＳ４２）、それぞれの初期値を第１線形フィードバックシフトレジスタ２ｔ、第２線形フィードバックシフトレジスタ３ｔ、および通信部９ｔへ供給する。

【００５３】

また、多項式係数生成部５ｔが、外部から入力される初期情報、あるいは予め定められた所定の条件に従って、第２線形フィードバックシフトレジスタ３ｔの特性多項式の係数s（$s_{n-1}, s_{n-2}, \cdots, s_2, s_1$）を生成し（ステップＳ４３）、第２線形フィードバックシフトレジスタ３ｔと通信部９ｔへ供給する。

【００５４】

第１線形フィードバックシフトレジスタ２ｔと第２線形フィードバックシフトレジスタ３ｔは、原始多項式選択部７ｔ、初期値生成部４ｔ、および多項式係数生成部５ｔから各初期値と係数が供給されると、各フリップフロップ回路とＡＮＤ回路に各初期値と係数を設定し、出力ビット数をカウントするカウンタｋの値をｋ＝０に設定する（ステップＳ４４）。第１線形フィードバックシフトレジスタ２ｔの各フリップフロップ回路$FA_{m-1}, FA_{m-2}, \cdots, FA_1, FA_0$には、初期値ia（$ia_{m-1}, ia_{m-2}, \cdots, ia_1, ia_0$）が設定され、各ＡＮＤ回路には、原始多項式選択部７ｔから供給された特性多項式の係数a（$a_{m-1}, \cdots, a_1$）が設定される。また、第２線形フィードバックシフトレジスタ３ｔの各フリップフロップ回路$FB_{n-1}, FB_{n-2}, \cdots, FB_1, FB_0$には、初期値ib（$ib_{n-1}, ib_{n-2}, \cdots, ib_1, ib_0$）が設定され、各ＡＮＤ回路には、特性多項式の係数s（$s_{n-1}, s_{n-2}, \cdots, s_2, s_1$）が設定される。なお、図３の第２線形フィードバックシフトレジスタ３ｔでは、$b_n=1, b_0=1$としているが、b_nおよびb_0にＡＮＤ回路を設けて、他の係数と同様に任意の値を設定できるようにしてもよい。

【００５５】

また、通信部９ｔは、原始多項式の識別番号、特性多項式の係数、および各初期値のそれぞれのビット値からなるイニシャルデータを生成し擬似乱数生成装置１Ｃｒへ送信する（ステップＳ４５）。この時、通信部９ｔは、所定の暗号化方式でイニシャルデータを暗号化して送信しても良い。

【００５６】

例えば、原始多項式の識別番号が２ビット（“10”）、初期値iaが７ビット（“1010101”）、初期値ibが８ビット（“11110000”）、特性多項式の係数sが７ビット（“0111011”）であった場合、イニシャルデータは２４ビットのデータ列（識別番号｜初期値ia｜初期値ib｜係数s）＝（101010101111100000111011）となる。

【００５７】

以降、擬似乱数生成装置１Ｃｔは、第１の実施形態（ステップＳ０４～ステップＳ１１）と同様の処理を行って擬似乱数r（$r_0, r_1, \cdots, r_{h-1}, r_h$）を出力する（ステップＳ４６～ステップＳ５１）。

【００５８】
一方、擬似乱数生成装置１Ｃｒの通信部９ｒは、擬似乱数生成装置１Ｃｔからイニシャルデータを受信すると（ステップＳ５２）、イニシャルデータから初期値ib（$ib_{n-1}, ib_{n-2}, \cdots, ib_1, ib_0$）と特性多項式の係数s（$s_{n-1}, s_{n-2}, \cdots, s_2, s_1$）とを抽出し、第２線形フィードバックシフトレジスタ３ｒに供給し、イニシャルデータから初期値ia（$ia_{m-1}, ia_{m-2}, \cdots, ia_1, ia_0$）を抽出し、第１線形フィードバックシフトレジスタ２ｒに供給し、イニシャルデータから原始多項式の識別番号を抽出し、原始多項式選択部７ｒに供給する。なお、受信したイニシャルデータが暗号化されている場合は、通信部９は、復号化してイニシャルデータを得る。

【００５９】
原始多項式選択部７ｒは、原始多項式の識別番号が供給されると、その識別番号に該当する原始多項式を原始多項式記憶部８ｒから１つ選択し（ステップＳ５３）、その選択した原始多項式の係数を特性多項式の係数a（$a_{m-1}, \cdots, a_1$）として第１線形フィードバックシフトレジスタ２ｒへ供給する。

【００６０】
また、第１線形フィードバックシフトレジスタ２ｒと第２線形フィードバックシフトレジスタ３ｒは、原始多項式選択部７ｒ、および通信部９ｒから各初期値と各係数が供給されると、各フリップフロップ回路とＡＮＤ回路に各初期値と係数を設定し、出力ビット数をカウントするカウンタｋの値をｋ＝０に設定する（ステップＳ５４）。

【００６１】
以降、擬似乱数生成装置１Ｃｒは、第１の実施形態（ステップＳ０４～ステップＳ１１）と同様の処理を行って擬似乱数r（$r_0, r_1, \cdots, r_{h-1}, r_h$）を出力する（ステップＳ５５～ステップＳ６０）。

【００６２】
このようにして、２つの擬似乱数生成装置１でイニシャルデータを共有することによって、同じ擬似乱数を生成することが可能となる。

【００６３】
なお、擬似乱数生成装置１は、上記の機能を記述した擬似乱数生成プログラムを汎用コンピュータに実行させることによって実現させても良い。この擬似乱数生成プログラムは、記録媒体から読み取られて汎用コンピュータに実行されても良いし、ネットワークを介して外部から伝送されて汎用コンピュータに実行されても良い。

【図面の簡単な説明】

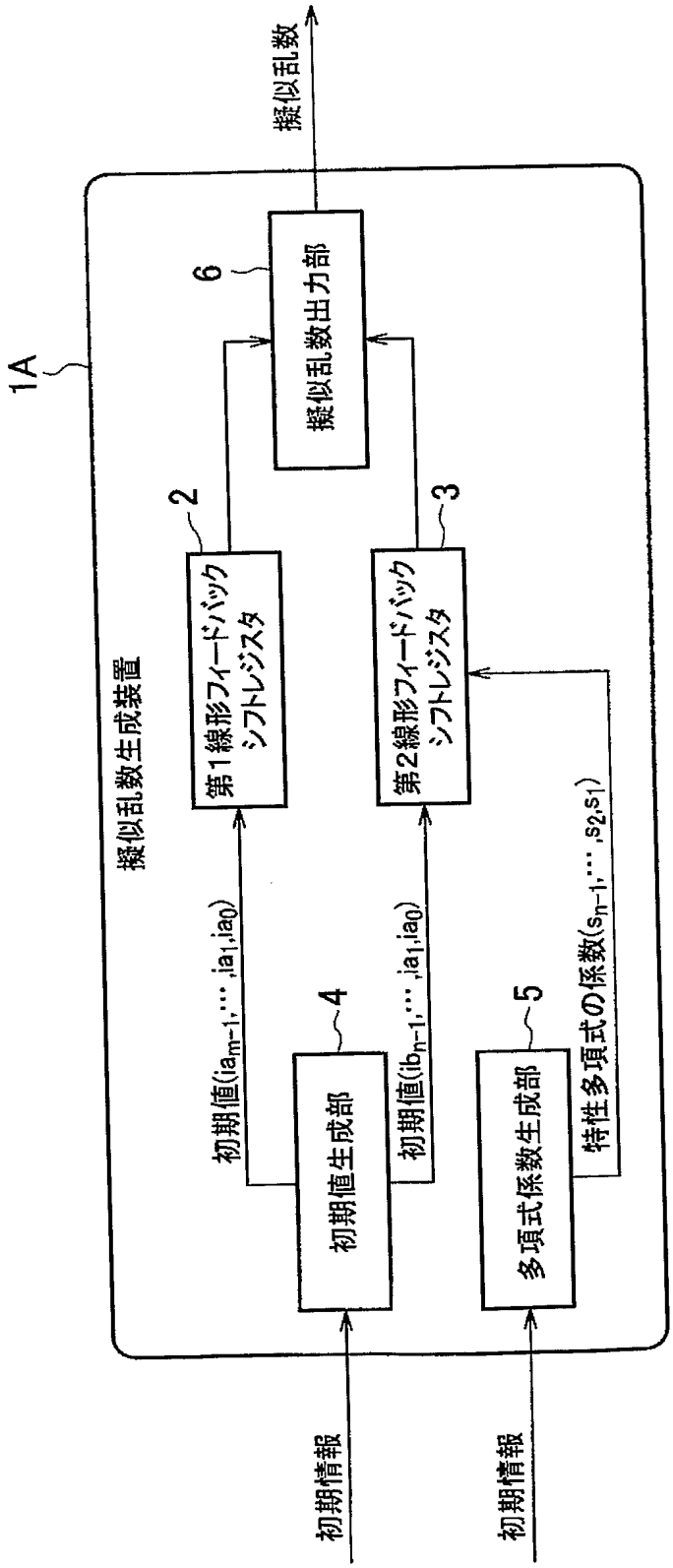
【００６４】
【図１】擬似乱数生成装置Ａの機能構成を示す図である。
【図２】第１線形フィードバックシフトレジスタの回路構成を示す図である。
【図３】第２線形フィードバックシフトレジスタの回路構成を示す図である。
【図４】第１の実施形態における擬似乱数生成の処理を示すフローチャートである。
【図５】第１線形フィードバックシフトレジスタと第２線形フィードバックシフトレジスタの値の遷移を示す図である。
【図６】擬似乱数生成装置Ｂの機能構成を示す図である。
【図７】第２の実施形態における擬似乱数生成の処理を示すフローチャートである。
【図８】擬似乱数生成装置Ｃの機能構成を示す図である。
【図９】第３の実施形態における擬似乱数生成の処理を示すシーケンス図である。

【符号の説明】

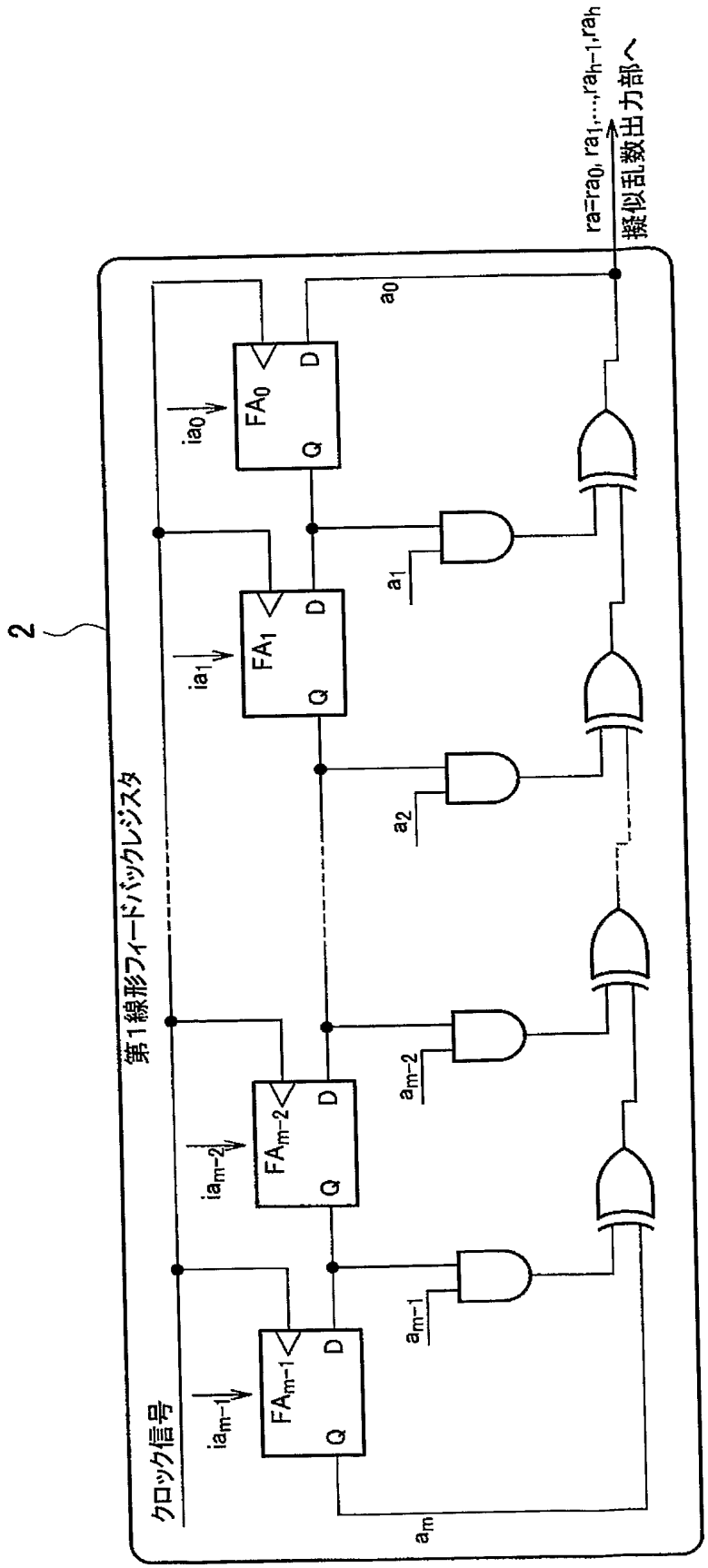
【００６５】
１Ａ、Ｂ、Ｃ　擬似乱数生成装置
２　第１線形フィードバックシフトレジスタ
３　第２線形フィードバックシフトレジスタ
４　初期値生成部
５　多項式係数生成部

6　擬似乱数出力部
7　原始多項式選択部
8　原始多項式記憶部
9　通信部

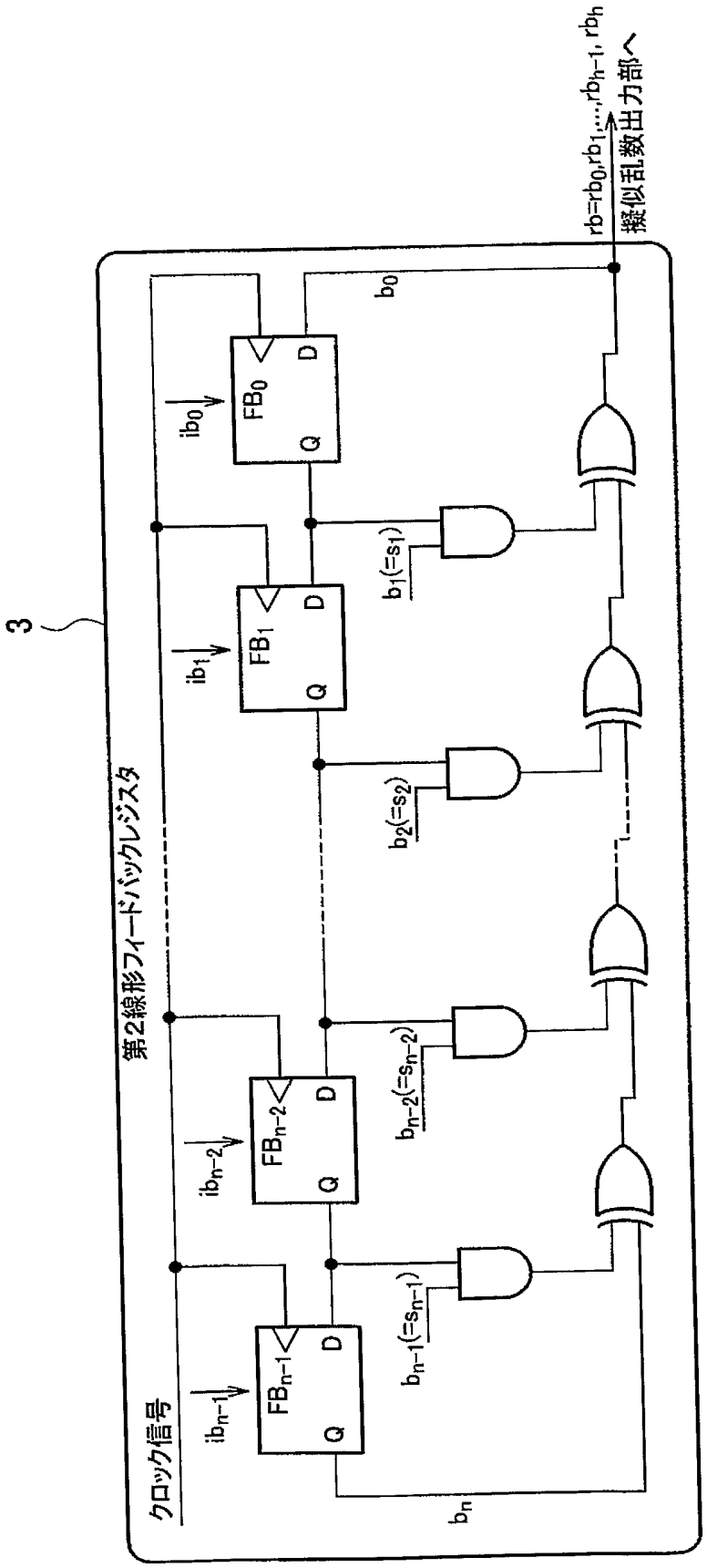
【書類名】図面
【図１】


擬似乱数
1A
擬似乱数生成装置
6
擬似乱数出力部
2
第1線形フィードバック
シフトレジスタ
3
第2線形フィードバック
シフトレジスタ
初期値(ia_{m-1},…,ia_1,ia_0)
初期値(ib_{n-1},…,ia_1,ia_0)
4
初期値生成部
5
多項式係数生成部
特性多項式の係数(s_{n-1},…,s_2,s_1)
初期情報
初期情報

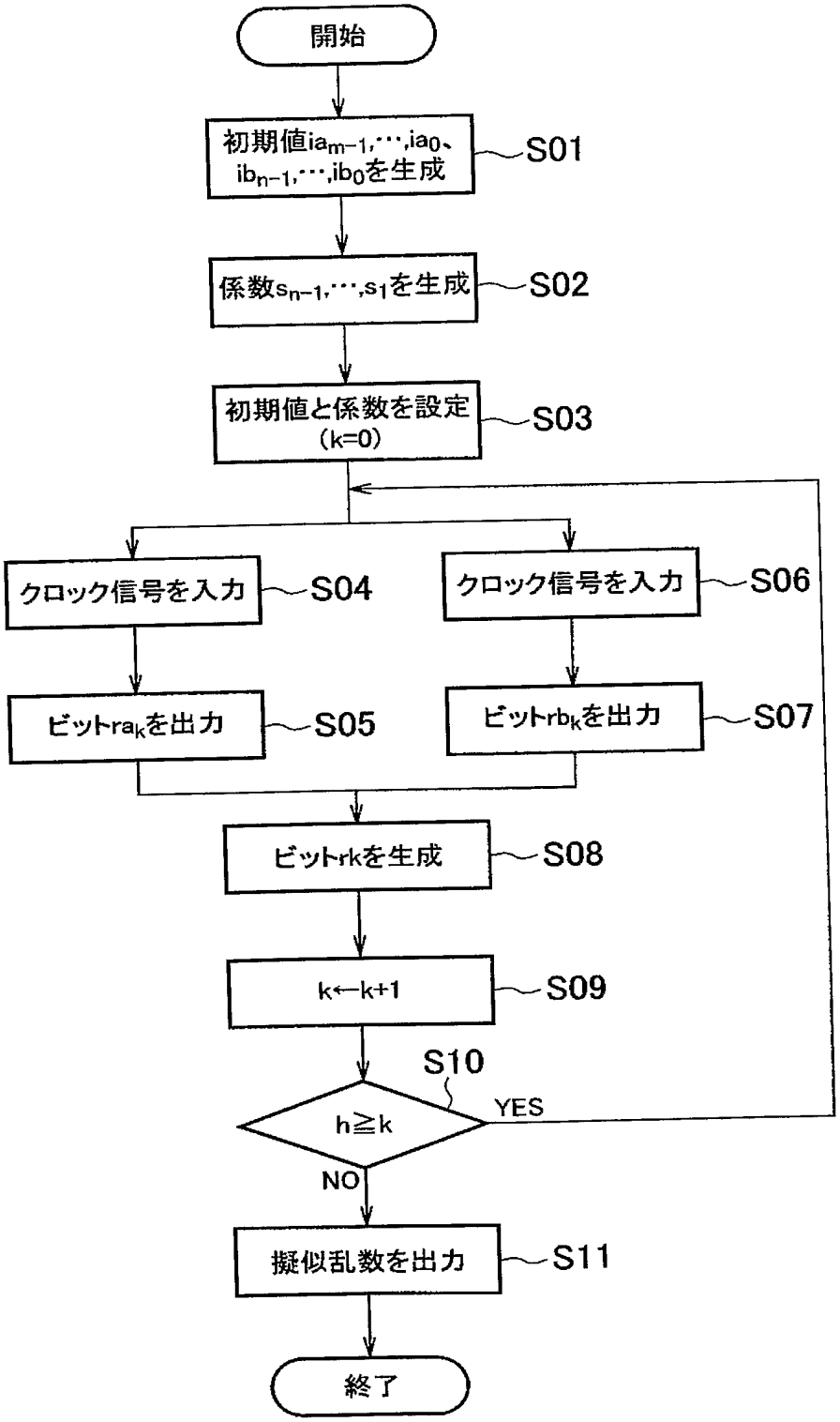
【図２】


2
第1線形フィードバックレジスタ
クロック信号
ra=ra0, ra1,...,ran-1,ran
擬似乱数出力部へ
FA0
FA1
FAm-2
FAm-1
ia0
ia1
iam-2
iam-1
a0
a1
a2
am-2
am-1
am

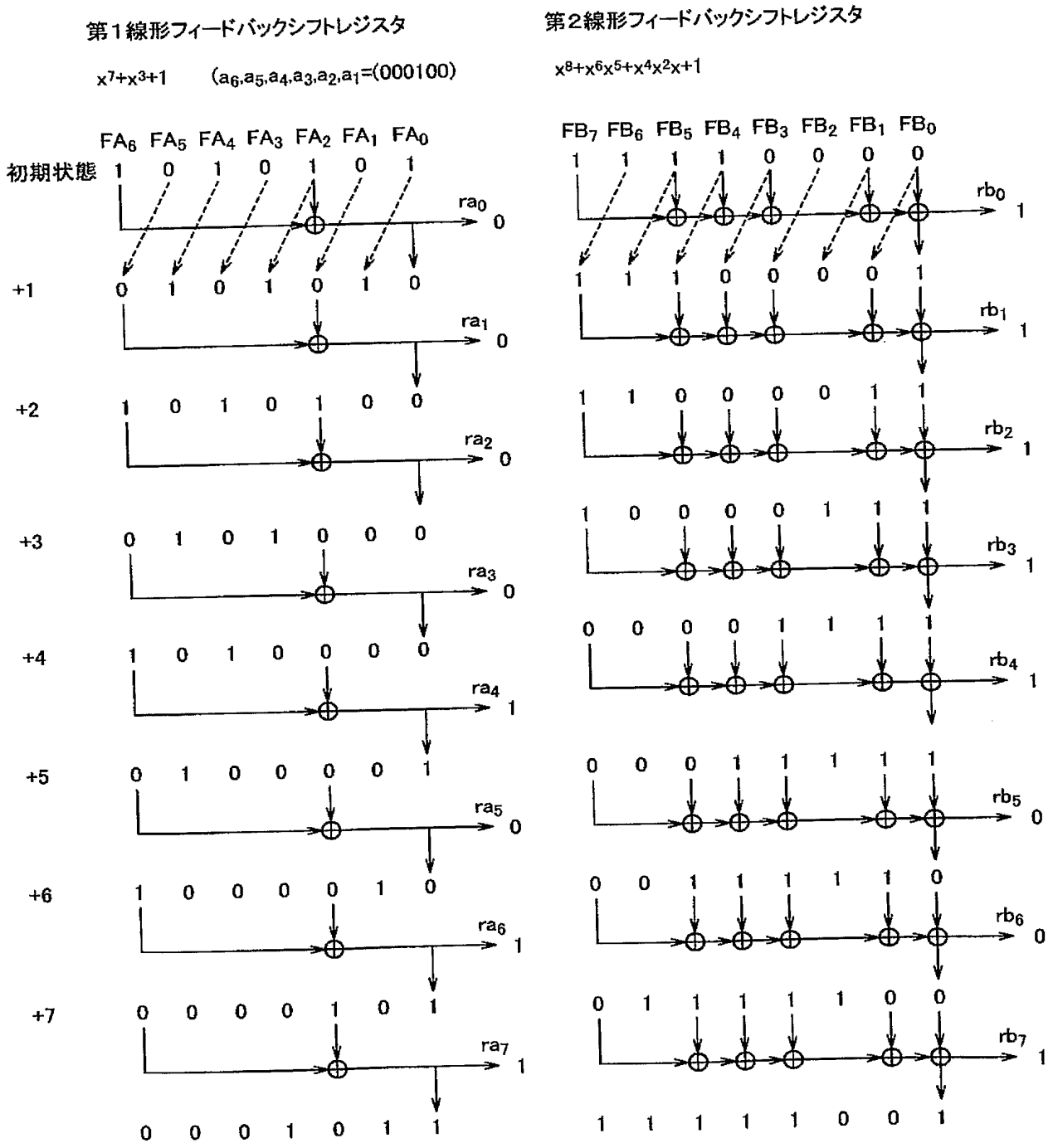
【図３】


3
第2線形フィードバックレジスタ
クロック信号
FB0
FB1
FBn-2
FBn-1
ib0
ib1
ibn-2
ibn-1
b0
b1(=s1)
b2(=s2)
bn-2(=sn-2)
bn-1(=sn-1)
bn
rb=rb0,rb1,...,rbh-1, rbh
擬似乱数出力部へ

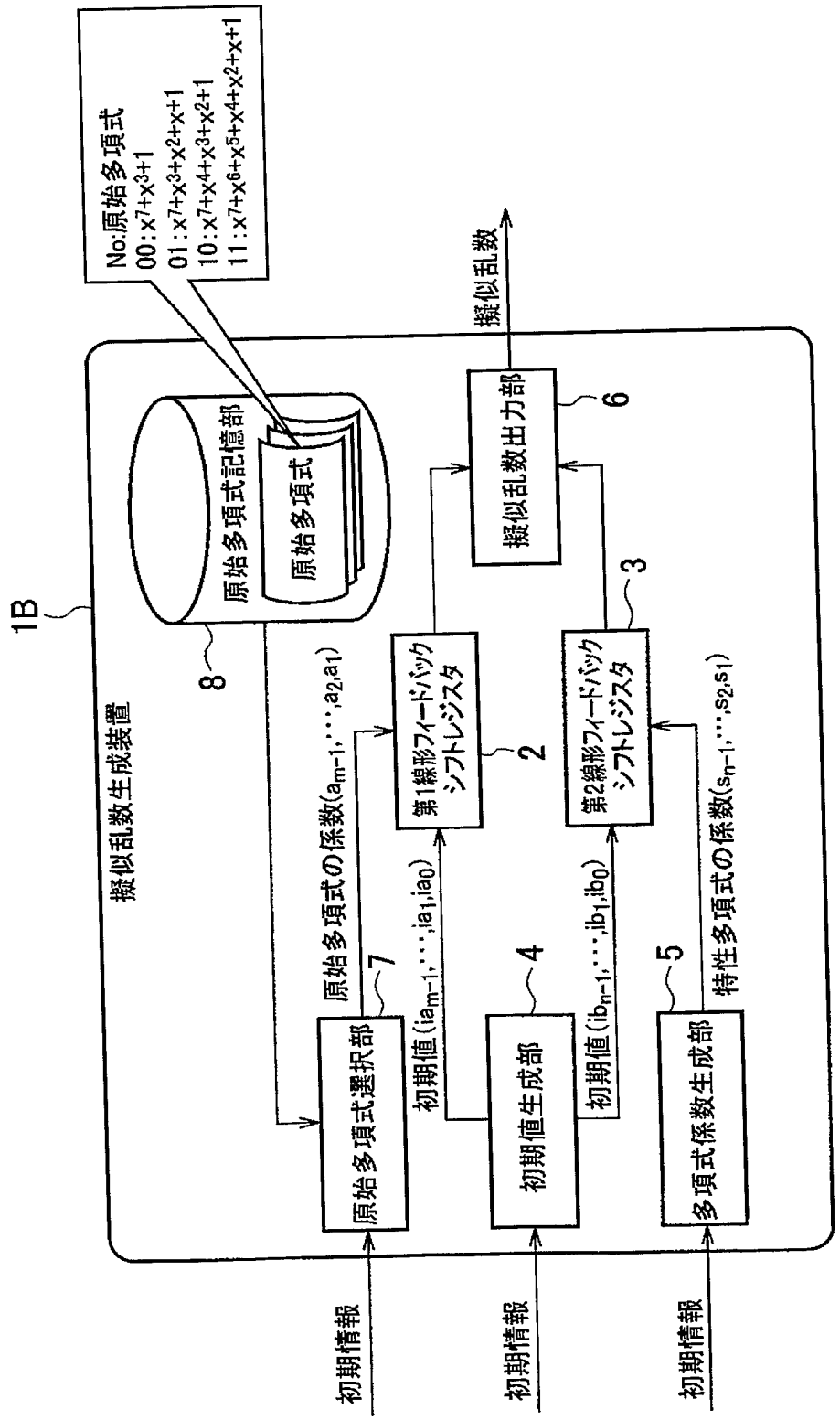
【図４】


開始
初期値$ia_{m-1},\cdots,ia_0$、$ib_{n-1},\cdots,ib_0$を生成
S01
係数$s_{n-1},\cdots,s_1$を生成
S02
初期値と係数を設定（k=0）
S03
クロック信号を入力
S04
ビットra_kを出力
S05
クロック信号を入力
S06
ビットrb_kを出力
S07
ビットrkを生成
S08
k←k+1
S09
S10
h≧k
YES
NO
擬似乱数を出力
S11
終了

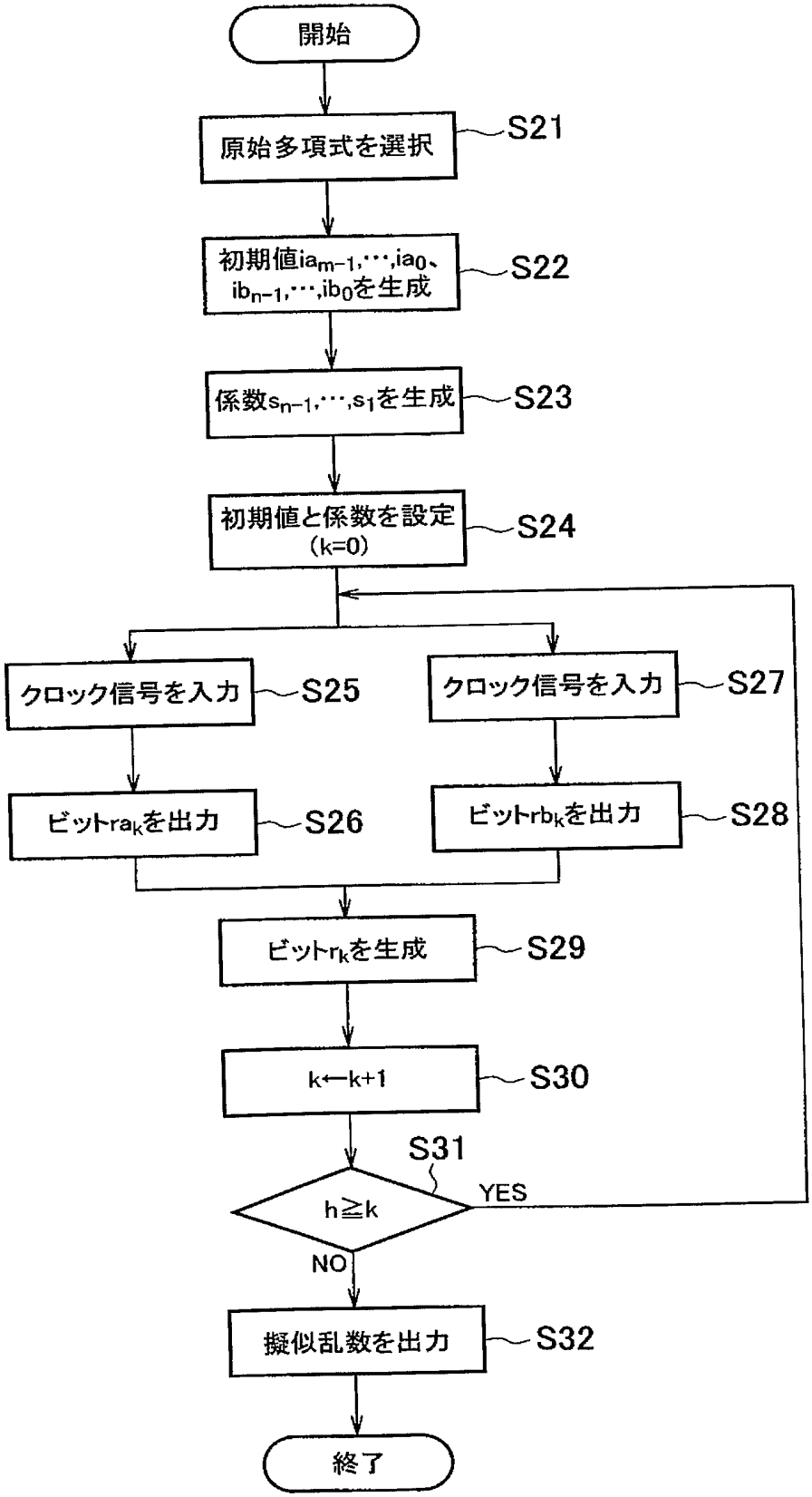
【図５】


第１線形フィードバックシフトレジスタ
x^7+x^3+1　$(a_6,a_5,a_4,a_3,a_2,a_1)=(000100)$
FA_6 FA_5 FA_4 FA_3 FA_2 FA_1 FA_0
初期状態 1 0 1 0 1 0 1
ra_0 0
+1 0 1 0 1 0 1 0
ra_1 0
+2 1 0 1 0 1 0 0
ra_2 0
+3 0 1 0 1 0 0 0
ra_3 0
+4 1 0 1 0 0 0 0
ra_4 1
+5 0 1 0 0 0 0 1
ra_5 0
+6 1 0 0 0 0 1 0
ra_6 1
+7 0 0 0 0 1 0 1
ra_7 1
0 0 0 1 0 1 1
第２線形フィードバックシフトレジスタ
$x^8+x^6x^5+x^4x^2x+1$
FB_7 FB_6 FB_5 FB_4 FB_3 FB_2 FB_1 FB_0
1 1 1 1 0 0 0 0
rb_0 1
1 1 1 0 0 0 0 1
rb_1 1
1 1 0 0 0 0 1 1
rb_2 1
1 0 0 0 0 1 1 1
rb_3 1
0 0 0 0 1 1 1 1
rb_4 1
0 0 0 1 1 1 1 1
rb_5 0
0 0 1 1 1 1 1 0
rb_6 0
0 1 1 1 1 1 0 0
rb_7 1
1 1 1 1 1 0 0 1

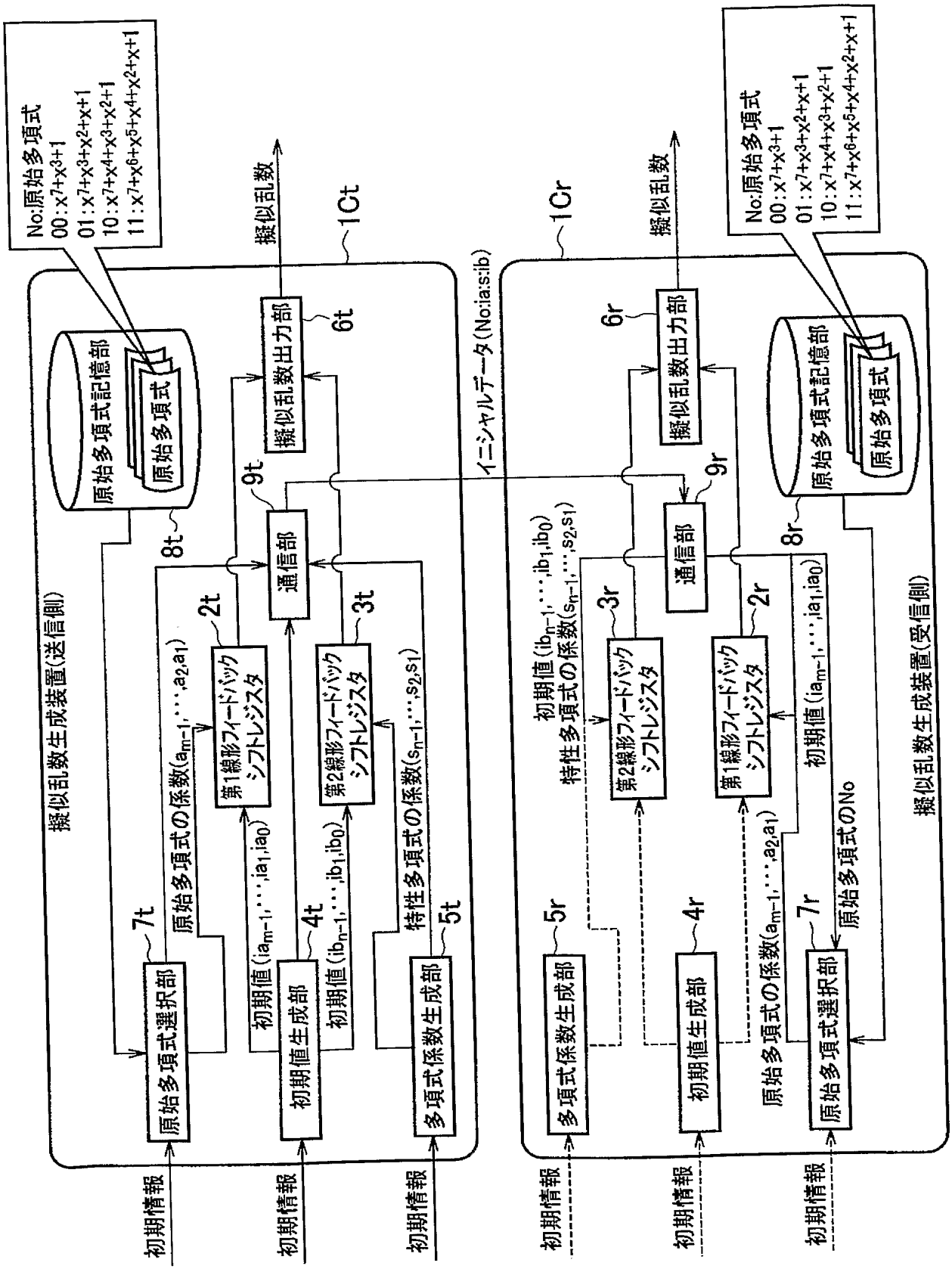
【図６】


No:原始多項式
00:x7+x3+1
01:x7+x3+x2+x+1
10:x7+x4+x3+x2+1
11:x7+x6+x5+x4+x2+x+1
擬似乱数
1B
擬似乱数生成装置
原始多項式記憶部
原始多項式
8
擬似乱数出力部
6
第1線形フィードバック
シフトレジスタ
2
第2線形フィードバック
シフトレジスタ
3
原始多項式の係数($a_{m-1},\cdots,a_2,a_1$)
7
初期値($ia_{m-1},\cdots,ia_1,ia_0$)
4
初期値($ib_{n-1},\cdots,ib_1,ib_0$)
5
特性多項式の係数($s_{n-1},\cdots,s_2,s_1$)
原始多項式選択部
初期値生成部
多項式係数生成部
初期情報
初期情報
初期情報

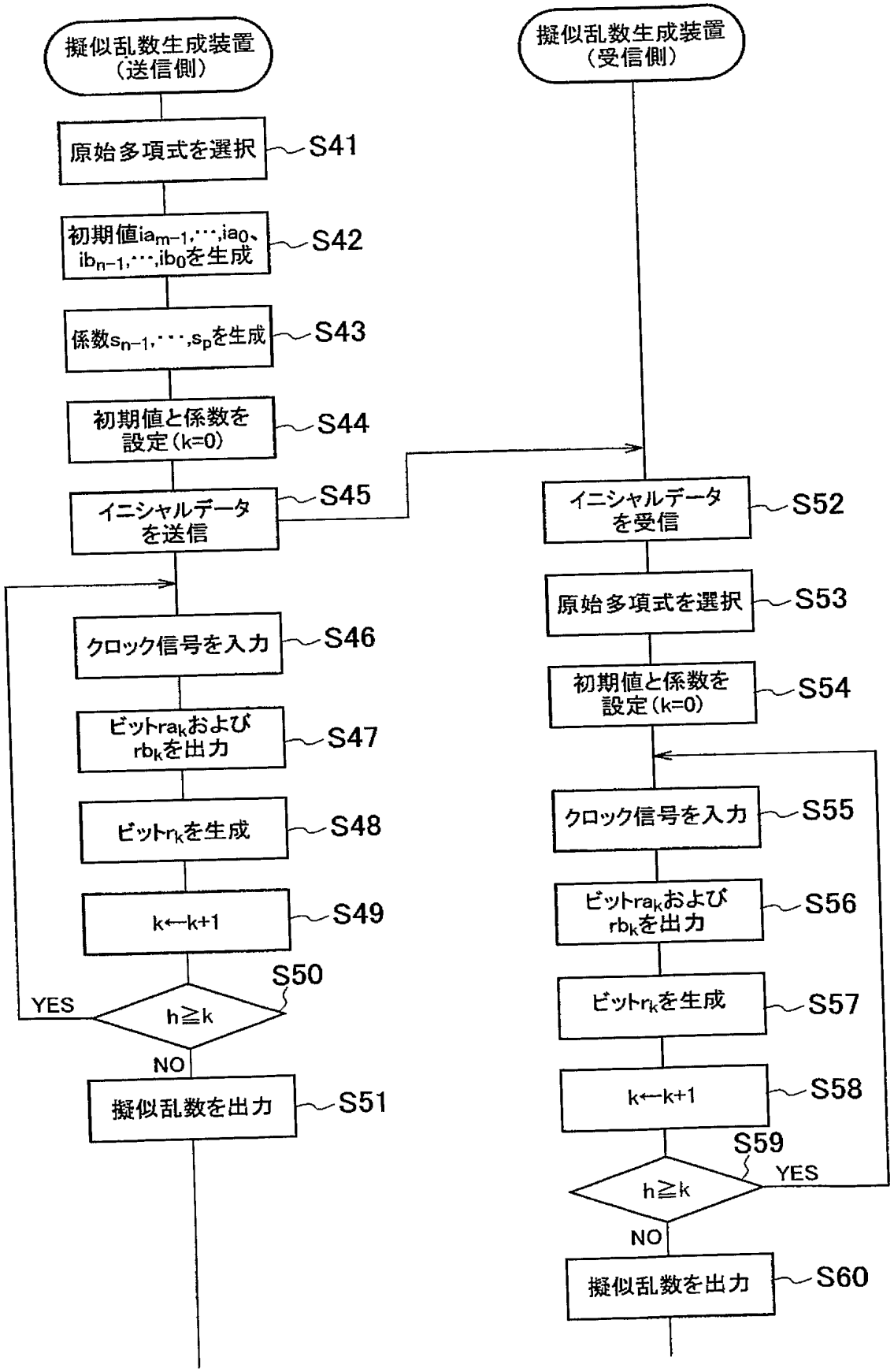
【図７】


開始
原始多項式を選択
S21
初期値$ia_{m-1},\cdots,ia_0$、$ib_{n-1},\cdots,ib_0$を生成
S22
係数$s_{n-1},\cdots,s_1$を生成
S23
初期値と係数を設定 (k=0)
S24
クロック信号を入力
S25
ビットra_kを出力
S26
クロック信号を入力
S27
ビットrb_kを出力
S28
ビットr_kを生成
S29
k←k+1
S30
S31
h≧k
YES
NO
擬似乱数を出力
S32
終了

【図８】


擬似乱数生成装置(送信側)
No:原始多項式
00:x7+x3+1
01:x7+x3+x2+x+1
10:x7+x4+x3+x2+1
11:x7+x6+x5+x4+x2+x+1
原始多項式記憶部
原始多項式
8t
擬似乱数
1Ct
6t
擬似乱数出力部
9t
通信部
イニシャルデータ(No:ia:s:ib)
原始多項式選択部
7t
原始多項式の係数($a_{m-1},\cdots,a_2,a_1$)
第1線形フィードバック
シフトレジスタ
2t
初期値($ia_{m-1},\cdots,ia_1,ia_0$)
初期値生成部
4t
初期値($ib_{n-1},\cdots,ib_1,ib_0$)
第2線形フィードバック
シフトレジスタ
3t
特性多項式の係数($s_{n-1},\cdots,s_2,s_1$)
多項式係数生成部
5t
初期情報
擬似乱数生成装置(受信側)
No:原始多項式
00:x7+x3+1
01:x7+x3+x2+x+1
10:x7+x4+x3+x2+1
11:x7+x6+x5+x4+x2+x+1
原始多項式記憶部
原始多項式
8r
擬似乱数
1Cr
6r
擬似乱数出力部
9r
通信部
初期値($ib_{n-1},\cdots,ib_1,ib_0$)
特性多項式の係数($s_{n-1},\cdots,s_2,s_1$)
第2線形フィードバック
シフトレジスタ
3r
第1線形フィードバック
シフトレジスタ
2r
初期値($ia_{m-1},\cdots,ia_1,ia_0$)
原始多項式の係数($a_{m-1},\cdots,a_2,a_1$)
原始多項式のNo
原始多項式選択部
7r
初期値生成部
4r
多項式係数生成部
5r
初期情報
初期情報
初期情報
初期情報

【図９】


擬似乱数生成装置（送信側）
原始多項式を選択
S41
初期値$ia_{m-1},\cdots,ia_0$、$ib_{n-1},\cdots,ib_0$を生成
S42
係数$s_{n-1},\cdots,s_p$を生成
S43
初期値と係数を設定（k=0）
S44
イニシャルデータを送信
S45
クロック信号を入力
S46
ビットra_kおよびrb_kを出力
S47
ビットr_kを生成
S48
k←k+1
S49
h≧k
S50
YES
NO
擬似乱数を出力
S51
擬似乱数生成装置（受信側）
イニシャルデータを受信
S52
原始多項式を選択
S53
初期値と係数を設定（k=0）
S54
クロック信号を入力
S55
ビットra_kおよびrb_kを出力
S56
ビットr_kを生成
S57
k←k+1
S58
h≧k
S59
YES
NO
擬似乱数を出力
S60

【書類名】要約書
【要約】
【課題】　擬似乱数列や送受信されるデータを観測されても、その後生成される擬似乱数列の推測が困難な暗号通信に好適な擬似乱数生成装置および擬似乱数生成プログラムを提供する。
【解決手段】　擬似乱数生成装置１は、第１線形フィードバックシフトレジスタ２、第２線形フィードバックシフトレジスタ３、初期値生成部４、多項式係数生成部５および擬似乱数出力部６を有し、初期値生成部４は、初期値を生成し、第１線形フィードバックシフトレジスタ２および第２線形フィードバックシフトレジスタ３へ供給し、多項式係数生成部５は、特性多項式の係数を生成して第２線形フィードバックシフトレジスタ３へ供給し、擬似乱数出力部６は、第１線形フィードバックシフトレジスタ２および第２線形フィードバックシフトレジスタ３から順次出力されるビット列とを基に、各ビットの排他的論理和から擬似乱数列を生成、出力する。
【選択図】　図１

特願２００４－０２３３３５

出　願　人　履　歴　情　報

識別番号　［０００００４３２９］

１．変更年月日　１９９０年　８月　８日
［変更理由］　新規登録
住　所　神奈川県横浜市神奈川区守屋町３丁目１２番地
氏　名　日本ビクター株式会社